Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of :	)	
Communications Assistance for	)	CC Docket No. 97 - 213
Law Enforcement Act	)	

Reply Comments of the Center for Democracy and Technology and Computer Professionals for Social Responsibility Regarding Implementation of the Communications Assistance For Law Enforcement Act (CALEA)

James X. Dempsey
CENTER FOR DEMOCRACY AND TECHNOLOGY
1634 I Street, N.W.
Washington, D.C. 20006
(202) 637-9800

Andy Oram
COMPUTER PROFESSIONALS FOR SOCIAL RESPONSIBILITY
P.O. Box 717
Palo Alto, CA 94302
(617) 499-7479
(650) 322-3778

February 11, 1998

TABLE OF CONTENTS

I. INTRODUCTION AND SUMMARY 1

II. BACKGROUND -- PRINCIPLES FOR INTERPRETING CALEA 3

A. In CALEA, as in other Wiretap-Related Laws, Congress Intended to Balance Law Enforcement, Privacy and Industry Interests. 3

B. Indeed, under CALEA, Law Enforcement Interests Are, in the Final Analysis, to Be Subordinated to Privacy and the Public Policy of Encouraging Technological Innovation. 4

C. The FBI's Push Now for Regulation of Carrier Practices and for Enhanced Surveillance Capabilities Is at Odds with the Evidence It Offered in 1994 in Justifying CALEA. 5

D. CALEA Was not Intended to Assure 100% Success of Law Enforcement Surveillance Activities 7

E. The FBI's Pursuit of a 100% Solution Has Resulted in Delays in Meeting Law Enforcement's Needs. 9

III. CARRIER SECURITY POLICIES AND PROCEDURES 9

A. CALEA Was Not Intended to Address All of the Problems that Could Potentially Affect Law Enforcement's Electronic Surveillance, and the Commission Should Reject the FBI's Effort to Turn CALEA into Such a Statute 9

B. For Good Reason, Federal Law Has Always Maintained an Arm's Length Relationship Between Telephone Companies and Law Enforcement in the Execution of Orders -- A Relationship That CALEA Was Not Intended to Change. 10

C. The FBI's Concerns about Timeliness and Review of Court Orders Are Best Handled, as They Have Been in the Past, by the Courts, under Section 2518(4) 12

D. Dangers of Human Compromise Are Not Unique to Digital Technologies and Are Not Within the Scope of CALEA. 12

IV. REASONABLY ACHIEVABLE AND EXTENSIONS OF THE COMPLIANCE DATE 13

V. PRIVACY AND SECURITY CONCERNS REMAIN UNADDRESSED 15

VI. CONCLUSION 16

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of :	)	
Communications Assistance for	)	CC Docket No. 97 - 213
Law Enforcement Act	)	

Reply Comments of the Center for Democracy and Technology and Computer Professionals for Social Responsibility Regarding Implementation of the Communications Assistance For Law Enforcement Act (CALEA)

I. INTRODUCTION AND SUMMARY

The FBI's approach to implementation of CALEA has strayed very far indeed from the issues the Bureau brought to Congress in 1994. A statute intended to ensure that advanced digital technology did not prevent law enforcement agencies from conducting wiretaps is now being cited by the FBI as the basis for this Commission to exercise rulemaking authority over non-technological aspects of surveillance operations, ranging from the personnel practices of telephone companies to their processing of surveillance orders. Meanwhile, the security concerns about the vulnerability of computerized surveillance functions that prompted Congress to enact Section 105 of CALEA are not receiving adequate attention.

The FBI's comments on the NPRM urge this Commission to institute rules regarding intrusive background checks of telephone company employees, limiting what companies can do to assure themselves of the validity of purported intercept orders, specifying the number of hours that could elapse before a surveillance is implemented, and requiring carriers to reassign employees outside normal personnel practices. These issues have nothing to do with the types of technological impediments to surveillance that CALEA was intended to address.

Ever since CALEA was passed, the FBI has tried to rewrite the statute administratively, acting as if Congress had enacted the law that had been proposed by the Bush Administration, which would have given the FBI the authority to dictate standards to the telecommunications industry. Congress rejected that approach, but the FBI continued to pursue it by attempting to dominate the industry standards process. Now, the FBI has gone back to an even earlier version of the legislation, which would have given this Commission primary authority over wiretap standards. Congress rejected that approach too. The Commission should decline the FBI's invitation to rewrite CALEA.

The duty of this Commission is to ensure that a balance is maintained among law enforcement, privacy and industry interests. Indeed, under CALEA, Congress made it clear that privacy interests and industry interests are paramount over law enforcement concerns.

CALEA is not a statute for all seasons. It was not intended to address anything and everything that could go wrong with an electronic surveillance. It was not a delegation to the Commission of general supervision over wiretap operations. It was intended to focus on technological impediments to electronic surveillance.

The Commission should reject the FBI's proposals to engage in extensive rulemaking on carrier personnel policies and on the handling of judicial orders. The technological concerns at the heart of CALEA are complicated enough and pose enough unresolved issues without the Commission's trying to solve all problems that may affect electronic surveillance. In section 105, Congress wanted to make sure that, in developing switch- or network-based solutions to the technological impediments to wiretapping, carriers did not create a new set of problems in the form of vulnerability to unauthorized surveillance. That should be the Commission's focus in this rulemaking.

In addition, under this docket number, or in a separate proceeding, the Commission should ensure that the statute is not used to expand law enforcement monitoring capabilities and that carriers are complying with section 103(a)(4)'s requirement to "protect[] the

privacy and security of communications and call-identifying information not authorized to be intercepted."

II. BACKGROUND -- PRINCIPLES FOR INTERPRETING CALEA

A. In CALEA, as in other Wiretap-Related Laws, Congress Intended to Balance Law Enforcement, Privacy and Industry Interests.

"For the past quarter century, the law of this nation regarding electronic surveillance has sought to balance the interests of privacy and law enforcement." Thus the House Judiciary Committee began its discussion of CALEA. H. Rpt. 103-827, p. 11.[1] The FBI now tries to ignore that quarter century of precedent. Indeed, the FBI tries to turn the law on its head, arguing that public safety and national security should be the paramount consideration in the Commission's interpretation of CALEA. FBI Comments, ¶ 96. This has never been our nation's approach to law enforcement authorities in general or to wiretapping in particular. Indeed, in specific reference to the wiretap laws, the Supreme Court has concluded that "the protection of privacy was an overriding congressional concern." Gelbard v. U.S., 408 U.S. 41, 48 (1972).

Specifically in CALEA, Congress did not give preeminence to law enforcement concerns. Rather, Congress clearly intended to strike a balance, adding the public interest in technological innovation to the two concerns that had informed the 1968 law. H. Rpt. 103-827, p. 13. As the Judiciary Committee report states:

> "Therefore, the bill seeks to balance three key policies: (1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies." H. Rpt. 103-827, p. 13.

---

[1] The Senate Judiciary Committee report is identical. S. Rpt. 103-402. No other committees filed reports. Thus, although some sections of the legislation changed after the Judiciary Committees acted, the Judiciary Committee reports remain the best legislative history. Many provisions were enacted unchanged from the version reported by the Judiciary Committees.

Ignoring the concept of balance, the FBI argues that the factors in CALEA "need to be weighed and applied in light of the critical importance to public safety of preserving law enforcement's electronic surveillance capabilities." FBI Comments, ¶ 91. Yet the effect on public safety is itself one of the very factors to be weighed. CALEA, section 109(b)(1)(A) - (K). Public safety cannot be both a factor to be weighed and a general qualifier that determines how each of the other factors is to be weighted. It is clear that Congress intended for the Commission to balance all of the factors.

B. Indeed, under CALEA, Law Enforcement Interests Are, in the Final Analysis, to Be Subordinated to Privacy and the Public Policy of Encouraging Technological Innovation.

The FBI's assertion that law enforcement trumps other interests is the exact opposite of what CALEA says. Congress decided that, if a technology or service cannot be reasonably modified to comply with CALEA, then carriers would nonetheless be able to deploy and use it. As the Committee report states, "if a service [or] technology cannot reasonably be brought into compliance with the interception requirements, then the service or technology can be deployed. This is the exact opposite of the original version of the legislation, which would have barred introduction of services or features that could not be tapped." H. Rpt. 103-827, p. 19.

In its comments, the FBI incorrectly states: "These goals [the comprehensive preservation and maintenance of electronic surveillance and related statutory search authority] are to be achieved through whatever technical modifications are necessary." ¶ 18. Again in ¶ 30 the FBI incorrectly suggests that CALEA requires carriers offering calling features "to make all necessary network modifications to comply with CALEA." These statements are flat wrong. CALEA only requires carriers to make changes that are reasonably achievable. As FBI Director Freeh testified in 1994, "The legislation reflects reasonableness in every provision." Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings on H.R. 4922 and S. 2375 Before the Subcomm. on Tech. and the Law of the Senate Comm. on the

Judiciary and the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary, 103rd Cong. (1994) (hereinafter "Hearings"), p. 113. With standards like "whatever technical modifications are necessary" and "all necessary modifications," the FBI is trying to ignore the testimony of Director Freeh and read reasonableness out of the statute.

Throughout the statute, it is clear that that law enforcement interests must yield to what is "reasonably achievable." Carriers are obligated to make available only such call-identifying data as is "reasonably available." CALEA, section 103(a)(2). This Commission may grant an extension of time for compliance if compliance within the specified period is "not reasonably achievable." Section 107(c). A court can order compliance only if alternative technologies or the facilities of another carrier are not "reasonably available" to law enforcement for implementing the interception and only if compliance is "reasonably achievable." Section 108(a). Carriers are not required to bear the costs of retrofitting equipment installed before January 1, 1995 if compliance is "not reasonably achievable." Section 109(b)(2). This is not a statute in which law enforcement interests are paramount.

C. The FBI's Push Now for Regulation of Carrier Practices and for Enhanced Surveillance Capabilities Is at Odds with the Evidence It Offered in 1994 in Justifying CALEA.

In determining how far the FBI approach to CALEA implementation has departed from Congress' intent, it is useful to look at the actual problems that were cited to Congress by the FBI as justification for the Act. Of the problems identified in 1994 by the FBI, the most common was lack of adequate capacity in cellular systems to accommodate multiple surveillances at the same time. This accounted for 30% of all problems law enforcement could identify in a series of surveys between 1992 and 1994. The second most common problem was the inability of certain cellular systems to provide law enforcement with call-identifying information on a real-time or contemporaneous basis. (The cellular systems collected dialing information, but there was a delay before the information could be

accessed.) The third most common set of problems related to special dialing features. When a person uses speed dialing, voice dialing or automatic redial or call-back, the pen register on the customer line only picks up the coded command, not the full number that it represents. The fourth most common problem was call forwarding: law enforcement could not capture incoming calls to the target's line that were forwarded at the central office using a service provided by the telephone company. See H. Rpt. 103-827, p. 15.

Based on this survey and statements of telephone company representatives, Congress enacted CALEA. And, of course, Congress was concerned to ensure that the future evolution of technology did not create new problems. But Congress did not intend to require a comprehensive redesign of the nation's telecommunications system. After all, of the tens of thousands of wiretaps, pen registers and traps and traces conducted in the 1992-94 timeframe, there had been only 183 documented problems.

Since 1994, even though CALEA implementation has been stalled and industry has continued to deploy digital equipment not designed with law enforcement's requirements in mind, electronic surveillance continues to be carried out. In the years since CALEA was enacted, the numbers of wiretaps, pen registers and trap and trace devices have remained at all-time highs, while the number of persons intercepted and the number of conversations monitored have gone up. See Wiretap Reports of the Administrative Office of the US Courts. This shows that there is no need for a comprehensive redesign of the nation's telecommunications networks.

The urgency expressed by the FBI when it sought enactment of CALEA is considerably belied by the tardiness of the FBI in addressing the capacity issue. While 30% of the problems identified by the FBI in 1994 involved lack of adequate capacity in cellular systems to accommodate multiple surveillances at the same time, the FBI has delayed for more than three years the issuance of a capacity notice that would be the first step in solving this problem.

Congress intended in CALEA to preserve the surveillance powers of the FBI and other law enforcement agencies. Congress did not require companies to maximize the surveillance potential of the new technology. FBI Director Louis Freeh testified repeatedly and consistently that the legislation was intended to preserve, not expand, the capability as it had existed since 1968. The House and Senate Judiciary Committee reports state that CALEA was intended "to *preserve a narrowly focused capability* for law enforcement agencies to carry out properly authorized intercepts" (emphasis added). H. Rpt. 103-827, p. 13.

D. CALEA Was not Intended to Assure 100% Success of Law Enforcement Surveillance Activities

Ever since CALEA was enacted, the FBI has sought a 100% solution -- a comprehensive examination of the nation's evolving telephone systems that would address all potential difficulties. The FBI has tried to identify all the permutations an interception could take, all the contingencies that might occur, all the bits of electronic information that it would be useful to have, and has tried to address each and every one of them. The FBI's goal has not been merely to prevent the loss of the wiretap *capability*, but to prevent the loss of *any bit* of potential electronic evidence.

This is not the approach that Congress adopted when it enacted CALEA. Ensuring a 100% solution is probably not possible, given the cleverness of some criminals and the rapid, ongoing evolution of technology. But even if it were, the effort would be fundamentally inconsistent with other societal goals, most notably the protection of privacy and the promotion of technological innovation.

FBI Director Freeh testified that CALEA was a comprehensive statute. He did not claim that it was absolutist. It was certainly intended to address all types of technological problems posed by digital telephony, not merely the immediate ones that were being experienced in 1994. Congress did not try to separately mandate a solution for cellular capacity and a solution for call forwarding and so on, although such a "band-aid" approach

was considered. Rather, the Congress set out four broad functional requirements that addressed advanced technology in general.

But Director Freeh also made it clear that CALEA did not promise a 100% solution to the difficulties posed by those technologies (let alone to the type of non-technological concerns that the FBI now raises). To the contrary, Freeh testified that the statute did not have total coverage: "We are missing a part of the playing field, but our position is that we don't want to miss the whole playing field." Hearings, p. 200.

Director Freeh admitted that there were cost constraints that might limit what the FBI would be able to do under the statute, and that if funds were not appropriated, then law enforcement would be satisfied with a partial solution:

> "My own view of that is that if this Congress, these committees made a finding that the cost/benefit of supplying further monies to a system which has been, perhaps, half-improved but not totally improved, if those fundings are no longer appropriate, then that money stops funding.
>
> I would still be in a better place if I could have access to half of the criminal conversations than none of the criminal conversations." Hearings, pp. 196-97.

Freeh also admitted that some targets would take steps to evade surveillance, and the legislation would not prevent that. Senator Leahy asked, "People, even people under surveillance, people on some occasions escape surveillance, or there is somebody else involved that law enforcement doesn't know about." Director Freeh responded, "That is absolutely correct. . . . There is a certain class of our targets, including spies, who are not going to be amenable to that [electronic surveillance]. That doesn't mean that we give up the whole universe of opportunity." Hearings p. 197

Director Freeh admitted that there would be technological impediments to surveillance:

> "There is always going to be and perhaps increasingly because of the technology developments, a range of criminal activity and a particular type of criminal actor who will be immune from the best-designed and best-built system." Hearings, p. 200.

Near the end of the hearings on the legislation, Freeh summed up: "what is left out is a totally ubiquitous or penetrating FBI compliance which will require every piece of

every network to . . . meet this requirement because actually, it is not necessary." Hearings, p. 203.

The FBI in 1994 was concerned with losing the wiretap capability entirely. Now it has shifted, and is asking for a 100% solution, the "totally ubiquitous compliance" that Director Freeh disavowed in 1994. Congress did not intended to give law enforcement 100% coverage and the Commission should not accept the FBI's efforts to impose it through rulemaking.

E. The FBI's Pursuit of a 100% Solution Has Resulted in Delays in Meeting Law Enforcement's Needs.

The FBI's pursuit of a 100% solution has resulted in a substantial delay in meeting the specific needs identified by the FBI in the 1994 hearings on CALEA. Even if manufacturers started designing to the interim standard today, it would be 18 to 24 months before switches could be deployed, beyond the October 1998 compliance date. Moreover, the ongoing negotiations with carriers and equipment manufacturers have probably delayed efforts to build to the interim standard, since everybody is waiting to see if additional capabilities are added as a result of the negotiations.

III. CARRIER SECURITY POLICIES AND PROCEDURES

A. CALEA Was Not Intended to Address All of the Problems that Could Potentially Affect Law Enforcement's Electronic Surveillance, and the Commission Should Reject the FBI's Effort to Turn CALEA into Such a Statute.

The FBI has strayed far indeed from the intent of CALEA, raising in its comments concerns about the proliferation of carriers, ¶ 3; the increasing centralization of telephone company security offices, ¶ 3; carrier scrutiny of judicial orders, ¶ 4; the number of carrier personnel involved in effecting intercepts, ¶ 8;[2] delays in reporting suspected compromises, ¶ 8; and "delays or flaws in a carrier's operational procedures for

[2] The FBI complains both that there are too few carrier personnel involved due to centralization, posing delay problems, ¶ 3, and too many, ¶ 8, increasing the risk to the security of intercepts.

responding to surveillance orders," ¶ 8. Almost as an afterthought the Bureau mentions the issue that prompted Congress to enact CALEA: "Further, in recent years, rapid advances in technology" have eroded law enforcement's surveillance capability. ¶ 5.

The non-technological procedural and personnel issues now raised by the FBI may be important, although the FBI's comments are remarkable for their hypothetical nature.[3] But none of these problems was addressed in CALEA. None of them is related to *digital* telephony or to any other technology for that matter. Indeed, they long predate consideration of CALEA.[4] In 1994, the FBI Director based his call for CALEA on the ground that lawful court orders had been "frustrated or delayed due to technology-based problems." Hearings p. 24. Consideration of the non-technological concerns now raised by the FBI is outside the jurisdiction of the Commission in this proceeding.

B. For Good Reason, Federal Law Has Always Maintained an Arm's Length Relationship Between Telephone Companies and Law Enforcement in the Execution of Orders -- A Relationship That CALEA Was Not Intended to Change.

When Title III was first enacted, it had no provision specifically requiring telecommunications carriers to assist law enforcement agencies in making approved interceptions. This led to some confusion, including a Ninth Circuit decision holding that, absent specific statutory authority, federal courts could not require carriers to assist lawful wiretaps. Application of the United States, 427 F.2d 639 (9th Cir. 1970). On July 29,

---

[3] In its comments, the FBI discusses problems that "could conceivably occur" as a result of improper or negligent conduct of carrier personnel. ¶ 37. It complains that delays in reporting a technical or human compromise "may" result in subjects becoming apprised that surveillance exists. ¶ 8. It notes " the possibility that critical evidence and information will be lost." ¶ 8. It notes that challenges to the admissibility that "could conceivably" be raised. ¶ 9.

[4] As long ago as 1976, the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance considered one of the issues raised by the FBI, the question of carriers closely scrutinizing wiretap orders, and found that the position of the companies was understandable: "As to . . . carriers who refused to comply with the original order on the basis that it was defective on its face, the Commission fails to see how they can be faulted in this regard. "Electronic Surveillance," Report of the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance (1976) p. 9; see also pp. 86-88.

1970, only two months after the Ninth Circuit decision, Congress amended the 1968 wiretap law to expressly require authorizing courts, upon government request, to order telephone company cooperation. The language was added to 18 U.S.C. §2518(4).

The practice of the phone companies under §2518(4) has always been to maintain a cooperative and consultative but arm's length relationship with law enforcement. In 1975 Congressional hearings on electronic surveillance, the attorney for AT&T, William Caming, who had represented AT&T in the drafting of Title III, testified:

> "In cooperating in court-ordered and national security cases, we endeavor to provide the very minimum assistance necessary to effectuate the particular wiretap. Under no circumstances do we do the wiretapping itself; that is the exclusive province of the appropriate law enforcement officers."

In CALEA, Congress was careful not to amend the §2518(4) duty. Instead, a reference to the CALEA enforcement provisions was "tacked onto" §2518(4), indicating that the two were separate. The Judiciary Committees' report confirms that CALEA did not change the existing assistance requirements:

> "The assistance capability and capacity requirements of the bill are in addition to the existing necessary assistance requirements in sections 2518(4) and 3124 of title 18, and 1805(b) of title 50. The Committee intends that 2518(4), 3124, and 1805(b) will continue to be applied, as they have in the past, to government assistance requests related to specific orders ... ." H. Rpt. 103-827, p. 20.

Accordingly, the FBI is wrong in reading into CALEA any change in the procedures -- and any authority for this Commission to regulate the procedures -- for complying with "specific orders."

For the first time ever, the FBI cites "anecdotal reports " of "instances" where carriers have refused to provide assistance to law enforcement. The FBI states that "the Commission has the opportunity, in furtherance of public safety, to establish rules in this proceeding that will minimize the likelihood of such case-by-case anomalies in the future." ¶33. These are not concerns that were presented to Congress, and are not within the scope of CALEA. The Committee report clearly indicates that "case-by-case anomalies" are to be dealt with "as they have in the past," under §2518(4), unaffected by CALEA.

C. The FBI's Concerns about Timeliness and Review of Court Orders Are Best Handled, as They Have Been in the Past, by the Courts, under Section 2518(4).

One illustration of how far the FBI has strayed from CALEA is its recommendation that the Commission should establish by rule what is the duty of a carrier upon receipt of a facially valid court order for an intercept. ¶ 34. Another is the Bureau's argument that the Commission should specify the time for implementing orders. ¶ 70. Congress has not delegated to the Commission authority to enter into these matters. These are matters to be worked out between law enforcement agencies and carriers. It is well known that the best way to ensure prompt implementation of an order is for law enforcement to notify the carrier while the application is still being processed. If this is done, an order can be implemented in a matter of minutes, not hours, as the FBI proposes.

The enforcement of surveillance orders is a matter for the judiciary. There is a considerable caselaw on the subject, one that it is unnecessary for the Commission to disrupt.

D. Dangers of Human Compromise Are Not Unique to Digital Technologies and Are Not Within the Scope of CALEA.

Many of the FBI's proposals for intrusive personnel security requirements hinge on the danger of compromise. ¶¶ 37 - 45. But the type of dangers to which the FBI refers are not unique to digital telephony, and are not unique to telephone companies. The FBI states a truism: that any carrier activities that threaten to compromise the security of electronic surveillance could endanger lives and impede prosecutions. It is equally true that any law enforcement activities that threaten to compromise the security of electronic surveillances activities could endanger lives and impede prosecutions. Any judicial activities that threaten to compromise the security of electronic surveillances activities could endanger lives and impede prosecutions. None of these were the concern of Congress in enacting CALEA. Congress focused in CALEA on the technological impediments to surveillance and the proper response to those technological impediments. The security of intercept operations was a concern only to the extent that changes made in to comply with CALEA might

heighten the insecurity of telecommunications systems. This was not a personnel security concern.

All that is necessary to compromise an interception is the knowledge of the identity of the target. The carrier employee who in prior times gave cable and pair information to law enforcement agencies for wiretapping was just as susceptible to being compromised as the carrier employee who activates the interception at a central switch. The technological innovations that are the focus of CALEA do not increase the likelihood that a surveillance will be compromised by an employee.

IV. REASONABLY ACHIEVABLE AND EXTENSIONS OF THE COMPLIANCE DATE

It is abundantly clear that compliance with CALEA is not reasonably achievable by the statutory deadline of October of this year. The FBI's recent implementation report to Congress states that one major manufacturer, Lucent, will not have a solution available until the third quarter of 1999. Another, Siemens, will not be able to deploy solutions until the first quarter of the year 2000, and will have to proceed in phases stretching into the following year. Nortel will have part of its solution ready by the third quarter of 1998, but the second phase will have to wait until the second quarter of the year 2000. The only company that will promise on the public record to have a solution ready by the third quarter of 1998 is Bell Emergis, and that solution appears to be speculative at best.

The only questions are: (1) how long an extension is appropriate; (2) will the FBI be able to exact from the industry additional concessions on the "punch-list" in return for agreeing to the extension; and (3) who bears the cost of bringing into compliance the huge embedded base of equipment installed after January 1, 1995? These questions are interrelated of course, since the more law enforcement surveillance capabilities are expanded with the detailed features sought by the FBI, the longer it will take to be reasonably achievable and the more it will cost.

The Commission should not promote a trade-off between a deadline extension and the incorporation of added capability from the punch-list. A solution that meets law enforcement needs but at the expense of privacy or innovation is not reasonably achievable.

The FBI has indicated it will accept an extension of compliance deadline (it really has no choice), but it is reluctant to pay for the costs of retrofitting existing equipment. It wants to put upon carriers the entire cost of retrofitting existing equipment once a solution is "readily achievable." This approach runs counter to the philosophy of CALEA, in which Congress intended to use the reimbursement mechanism to force law enforcement to make priorities, and to bring the cost of compliance into the public view.

The FBI is trying to avoid the public accountability that Congress made a centerpiece of the CALEA balance. The FBI has made it clear that it will delay compliance, but only if carriers agree to the added capabilities. This is going outside the CALEA process. It also leaves open the question of who pays. The FBI would like to put onto carriers as much of the cost of CALEA compliance as possible. This saves the taxpayer money, but it hides the true cost of CALEA compliance. It denies the Congress and the public the ability top oversee FBI expenditures for compliance. It lessens the likelihood of a prioritization of needs.

The NPRM raises the relationship between a section 107 determination of what is reasonably achievable in terms of extending the deadline and the section 109 determination of what is reasonably achievable in terms of reimbursement for retrofitting embedded base. Section 107 requires a two-step inquiry. First, it must be asked whether compliance technology is available. If it is not, the inquiry ends, and the extension must be granted. In that regard, the factors in section 109 are irrelevant: if the technology is not available, an extension must be granted until it is available. If the technology is "available," there must be a further inquiry as to whether its application is reasonably achievable. Even if technology is available, compliance might not be reasonable. In that regard, the factors in section 109 are relevant: even after compliance technology is available, compliance is not

"reasonably achievable" if it means substantial burden on carriers or substantial interference with privacy. If something is not available, it is not achievable. But once it becomes available, it still may not be reasonable to expect the carriers to install it at their own cost.

V. PRIVACY AND SECURITY CONCERNS REMAIN UNADDRESSED

The Commission has yet to confront the privacy concerns raised by the FBI's demands for added surveillance capabilities. Last year, it may have made sense for the Commission to wait and see if industry and the FBI could "work something out." But it is clear that the FBI is trying to use delay to force industry to accept added capabilities.

Contrary to the intent of Congress, which wanted the telephone industry to decide how to satisfy certain basic surveillance requirements, the FBI tried to dominate the implementation process, insisting that companies include in their systems features that would give the government more comprehensive surveillance capabilities. Under pressure from the FBI, the wireless phone industry agreed to provide law enforcement with the capability to track the location of cellular phone users.

Industry has also agreed that carriers using increasingly common "packet switching" protocols may provide to the government the full content of customer communications when the government is only authorized to intercept the less sensitive addressing data that indicates who is calling whom. The standard was modified in response to concerns raised by CDT and certain companies, but it is unclear whether the modification addresses the issue adequately.

Switch-based solutions adopted under CALEA may increase the likelihood that a surveillance will be compromised by a hacker obtaining access to the surveillance administration system. This past Sunday's New York Times contained an article illustrating the problems we are concerned about, noting "the risks inherent in the increasingly widespread reliance on computers and computer networks." Markoff, "Design Flaw in Security Systems Leaves Airports Vulnerable to Terrorists, Officials Say,

New York Times, February 8, 1998, p. 20. The context there was different, but the concern with reliance on networked computers is the same. That is why we have urged greater attention to systems security.

VI. CONCLUSION

What started as a legislative effort to ensure that advanced digital technology did not prevent law enforcement agencies from conducting wiretaps is now snarled in FBI efforts to use the new technology to enhance its surveillance capabilities and to enlist this Commission in regulating a wide range of carrier practices. The impact on privacy has been overshadowed by concerns about extending the statute's October 1998 compliance deadline, by disputes over who pays for switching equipment upgrades to meet government demands, and now by proposals to institute intrusive background check requirements for carrier personnel.

The NPRM comments of the FBI represent its boldest effort yet to rewrite CALEA. The FBI tries to raise before the Commission issues not only outside the scope of the concerns before Congress when it enacted CALEA, but directly at odds with the concerns that prompted Congress to enact CALEA. The Commission should reject the FBI's efforts. They are not supported by either the text of the statute or by the legislative record. They would take this Commission into areas properly left to the judicial branch (the enforcement of wiretap orders) and they would involve the Commission in supervision in intercept operations. Telephone companies are not part of the government. There should be an arm's length relationship.

The FCC should use its current NPRM to assure itself of the security of the networked surveillance administration systems that carriers will be installing to comply with CALEA, consulting if necessary with computer security experts. The FCC should drop its proposals for intrusive background investigations of carrier personnel. The FCC

should launch an inquiry into the privacy implications of surveillance in a packet switching environment.

CALEA is not a statute for all seasons. It was not intended to address anything and everything that could go wrong with a surveillance. It was not a delegation of general supervision of wiretap operations. It was intended to focus on technological concerns. In section 105, Congress wanted to make sure that, in developing solutions to the technological concerns, carriers did not create a new set of problems. That should be the Commission's focus in this rulemaking.

Respectfully submitted,

James X. Dempsey
CENTER FOR DEMOCRACY
AND TECHNOLOGY
1634 I Street, N.W.
Washington, D.C. 20006
(202) 637-9800

Andy Oram
COMPUTER PROFESSIONALS FOR
SOCIAL RESPONSIBILITY
P.O. Box 717
Palo Alto, CA 94302
(617) 499-7479
(650) 322-3778

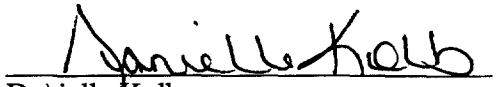
Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of	)	
	)	
Communications Assistance for	)	CC Docket No. 97-213
Law Enforcement Act	)	

Certificate of Service

I, Danielle Kolb, the Office Administrator for the Center for Democracy and Technology (CDT), 1634 Eye Street NW, Suite 1100, Washington, District of Columbia 20006, hereby certify that, on February 11, 1998, I caused to be served, by hand, copies of the **CDT's and CPSR's Reply Comments On Communications Assistance for Law Enforcement Act,** the original of which is filed herewith, upon the parties identified on the attached service list.

DATED at Washington, District of Columbia this 11th day of February, 1998.



Danielle Kolb

The Honorable William E. Kennard
Federal Communications Commission
Room 814
1919 M Street, NW
Washington, DC 20554

The Honorable Gloria Tristani
Federal Communications Commission
Room 826
1919 M Street, N.W.
Washington, DC 20554

The Honorable Michael K. Powell
Federal Communications Commission
Room 844
1919 M Street, N.W.
Washington, DC 20554

The Honorable Harold Furchtgott-Roth
Federal Communications Commission
Room 802
1919 M Street, N.W.
Washington, DC 20554

The Honorable Susan P. Ness
Federal Communications Commission
Room 832
1919 M Street, N.W.
Washington, DC 20554

A. Richard Metzger, Jr
Federal Communications Commission
Room 500
1919 M Street, N.W.
Washington, DC 20554

Kent R. Nilsson
Federal Communications Commission
Room 812
1919 M Street, N.W.
Washington, DC 20554

Geraldine Matise, Chief
Network Services Division
Common Carrier Bureau
Federal Communications Commission
2000 M Street N.W. - Room 235A
Washington, Dc 20554

International Transcription Service, Inc.
2100 M Street, N.W., Suite 140
Washington, DC 20037